AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method of encryption of data in a digital television system communicated between a first decoder and a portable security module operatively connected to the first decoder on a receiving side of the digital television system, comprising:

storing ~~wherein at least one~~ a plurality of precalculated key pairs ~~is stored~~ in a memory of the first decoder, each of said ~~at least one~~ plurality of precalculated key pairs comprising a session key and an encrypted ~~version of the~~ session key prepared using a transport key,

selecting and processing at least one session key to generate a definitive session key, wherein the definitive session key is generated by repeatedly encrypting an initial session key value known to both the first decoder and the portable security module in both devices using an ordered sequence of session keys and an encryption algorithm sensitive to an order of encryption; and

communicating the ordered sequence of session keys and an encrypted version of said at least one session key to the portable security module,

~~the encrypted version of the session key being subsequently communicated to the portable security module~~ wherein the portable security module is configured to ~~which~~ use the ordered sequence of session keys and the transport key to decrypt[[s]] the encrypted version of the at least one session key ~~using an equivalent transport key~~ to obtain the definitive session key,

wherein the transport key is stored in [[its]] a memory associated with the portable security module;

wherein ~~such that~~ data communicated from at least the portable security module to the first decoder may thereafter be encrypted and decrypted by the definitive session key.

2. (Canceled)

3. (Currently Amended) A method as claimed in claim [[2]] 1 in which a subset of a plurality of stored session keys is chosen by the first decoder to generate the definitive

session key, the associated encrypted versions of the subset of session keys being communicated to the portable security module for decryption and processing.

4. (Canceled)

5. (Canceled)

6. (Previously Presented) A method as claimed in claim 1 in which said at least one precalculated key pair is selected from a larger set of precalculated key pairs prior to being stored in the first decoder.

7. (Currently Amended) A method as claimed in claim 1 in which the encrypted version of a session key communicated to the portable security module also includes a signature value readable by the portable security module to verify the authenticity of the encrypted ~~version of the~~ session key.

8. (Previously Presented) A method as claimed in claim 1 in which an algorithm and transport key used to encrypt and decrypt a session key correspond to a symmetric algorithm and associated symmetric key.

9. (Previously Presented) A method as claimed in claim 1 in which an encryption algorithm used with a session key to encrypt and decrypt data communicated between the first decoder and the portable security module corresponds to a symmetric algorithm.

10. (Canceled)

11. (Canceled)

12. (Previously Presented) A method as claimed in claim 1, in which the portable security module corresponds to one of a smart card and a conditional access module.

13. (Previously Presented) A method as claimed in claim 1, in which the first decoder corresponds to a conditional access module and the portable security module corresponds to a smart card.

14. (Previously Presented) A method as claimed in claim 1, in which data encrypted and decrypted with the session key corresponds to control word data.

15. (Previously Presented) A method as claimed in claim 1, in which data encrypted and decrypted with the session key corresponds to descrambled broadcast data.

16. (Canceled)

17. (Previously Presented) A method as claimed in claim 1 as applied to a home network system, wherein the first decoder and the portable security module correspond to consumer electronic devices adapted to transfer data via a communication link.

18. (Canceled)

19. (Canceled)

20. (Canceled)

21. (Currently Amended) A digital television system for providing secure communication of data ~~between a first decoder and a portable security module~~, comprising:

a first decoder comprising:

a memory for storing a plurality of precalculated key pairs, wherein each of the plurality of precalculated key pairs comprises a session key and an encrypted session key prepared using a transport key;

a means for selecting and processing at least one session key to generate a definitive session key, wherein the definitive session key is generated by repeatedly encrypting an initial session key value known to both the first decoder and a portable security module using an ordered sequence of session keys and an encryption algorithm sensitive to an order of encryption; and

communicate the ordered sequence of session keys and an encrypted version of said at least one session key to the portable security module;

the portable security module operatively connected to the first decoder on a receiving side of the digital television system comprising:

a memory for storing the transport key;

means for decrypting the encrypted version of said at least one session key using the transport key and the ordered sequence of session keys to obtain the definitive session key; and

means for encrypting data using the definitive session key, wherein the encrypted data is communicated using a communication means to said first decoder ~~,said first decoder comprising a memory for storing at least one precalculated key pair comprising a session key and an encrypted version of the session key prepared using a transport key, and~~

~~communication means for communicating the encrypted version of the session key to said portable security module, said portable security module comprising a memory for storing an equivalent transport key, decryption means for decrypting said encrypted version of the session key using said equivalent transport key, and means for encrypting data to be communicated to said first decoder using said session key~~.

22. (Canceled)

23. (Currently Amended) A system as claimed in claim 21, in which the encrypted version of a session key includes a signature value readable by the portable security module to verify the authenticity of the encrypted ~~version of the~~ session key.

24. (Previously Presented) A system as claimed in claim 21, in which an algorithm and transport key used to encrypt and decrypt a session key correspond to a symmetric algorithm and associated symmetric key.

25. (Previously Presented) A system as claimed in claim 21, in which an encryption algorithm used with a session key to encrypt and decrypt data communicated between the first decoder and the portable security module corresponds to a symmetric algorithm.

26. (Canceled)

27. (Canceled)

28. (Previously Presented) A system as claimed in claim 21, in which the portable security module corresponds to one of a smart card and a conditional access module.

29. (Canceled)

30. (Canceled)

31. (Previously Presented) A system as claimed in claim 21 as applied to a home network system, wherein the first decoder and the portable security module correspond to consumer electronic devices adapted to transfer data via a communication link.

32. – 33. (Canceled)